

Error correction for mutually interacting qubits

Julio Gea-Banacloche

Department of Physics, University of Arkansas, Fayetteville, AR 72701

(February 1, 2008)

Abstract

For a simple model of mutually interacting qubits it is shown how the errors induced by mutual interactions can be eliminated using concatenated coding. The model is solved exactly for arbitrary interaction strength, for two well-known codes, one and two levels deep: this allows one to see under which circumstances error amplitudes add coherently or incoherently. For deeper concatenation, approximate results are derived which make it possible to calculate an approximate “threshold” value for the product of interaction strength and free evolution time, below which the failure probability for an encoded qubit decreases exponentially with the depth of the encoding. The results suggest that concatenated coding could fully handle the errors arising from mutual interactions, at no extra cost, in terms of resources needed, from what would be required to deal with random environmental errors.

03.67.Lx, 89.70.+c, 89.80.+h

I. INTRODUCTION AND MODEL

In previous papers [1,2] I have discussed how unwanted mutual interactions between qubits can be a source of error in a quantum computer (or quantum memory register) and studied some of the characteristic features of this type of error. It was found in [1] that, if the characteristic interaction energy is $\hbar\delta$, the fidelity \mathcal{F} of the register decreases with time t and with the total number of qubits N as

$$\mathcal{F} \sim e^{-N(\delta t)^2} \quad (1)$$

Equation (1) suggests that $(\delta t)^2$ can be interpreted as a sort of failure probability per qubit. In [2] it was shown that the general scaling (1) with t holds even when the register is being acted on by “gates” such as one might use in the course of a quantum computation: that is, the error accumulates quasi-coherently in time, and there is no “quantum Zeno effect” associated with normal gate operation. (This suggests, in particular, that it is not necessary to simulate a full computation to estimate the magnitude of this effect; instead, it should be enough to calculate the survival probability of an appropriate initial state of the register under the action of the appropriate Hamiltonian [3].)

Mutual interactions are Hamiltonian and hence, in principle, reversible, and there exists, in fact, a variety of special techniques for eliminating, or greatly reducing, these errors: in particular, techniques similar to, and inspired by, the use of refocusing pulses in magnetic resonance [4,5]. Nonetheless, it is worthwhile to look at the question of how well these errors could be eliminated by the use of ordinary error-correction methods based on quantum error-correcting codes [6,7], and in particular on concatenated coding, if only because one would like to be able to make an informed choice between various available methods. Moreover, although pulse methods could in principle be used to deal with certain kinds of environmental noise, it seems very likely that, in large-scale implementations of quantum computers, error-correcting codes will have to be used, in any event, to deal with at least some of these random environmental errors. Assuming, then, that these codes would already be in place, it is natural to ask how much one could get from them.

While there is no question that the present theory of quantum error-correction codes covers mutually interacting qubits as a special case, this is not a case that is often explicitly discussed, and, in particular, it is not immediately clear whether, in order to obtain a threshold estimate for these kinds of errors one should add them coherently (adding error amplitudes) or incoherently (adding error probabilities). This is one of the issues explored in this paper, for the two best-known quantum error-correcting codes: the 5-qubit and 7-qubit codes, and their concatenated forms. The conclusion, at least for the kind of interaction Hamiltonian assumed, is that these codes could fully handle the errors arising from mutual interactions, almost certainly at no extra cost in terms of resources needed (e.g., depth of concatenation). This is an encouraging result which may not have been immediately obvious before.

The interaction to be considered here is one that results in pure phase shifts, conditioned on the relative state of neighboring qubits, according to a Hamiltonian

$$H = \sum_{n=1}^{N-1} \hbar\delta\sigma_{zn}\sigma_{z,n+1} \quad (2)$$

Examples of physical systems leading to interactions of this form have been discussed in previous publications [1,2]; in [2] it has also been shown that, for instance, changing σ_z to σ_x (bit errors instead of phase errors) does not modify substantially the scaling (1).

In order to simplify the calculation, the (unrealistic) assumption is made that the qubits are divided into physical blocks, each of length N_c , which do not interact with each other; that is, the interaction Hamiltonian is applied separately to each such block. The blocks are intended to represent the “logical” qubits in a computer encoded for error correction. When the code is concatenated, the decoupling assumption is applied at the lowest (deepest) level: For instance, for a code concatenated once, a logical qubit is made of $N_c \times N_c$ physical qubits, and it is assumed that the N_c lowest-level blocks do not interact with each other. While unrealistic, it is expected that this approximation should not modify the results very much, based on the numerical calculations made using a similar “decoupling of registers” approximation in ref. [2].

In the following Section, the action of this Hamiltonian on a register encoded for error correction is analyzed, and then in Section III the analysis is extended to a concatenated code. The goal is to derive an expression for the “failure probability” per qubit, that is to say, the probability that the evolution under the Hamiltonian (2) may lead to a state which cannot be recovered by the error-correction protocol. Section II shows a few general features of this failure probability, such as its dependence on the initial state considered, and the way some error amplitudes add coherently and some do not, depending on the code considered. These results pave the way for the more complicated situation discussed in Section III. It is to be noted that the failure probability is calculated here for arbitrarily large interaction strength, for up to two-level-deep concatenated codes.

II. RESULTS FOR SIMPLE DISTANCE 3 CODES

Distance 3 codes can correct any of the three basic one-qubit errors represented by the three Pauli matrices σ_x , σ_y , and σ_z . They will typically fail whenever two errors happen simultaneously in the same logical block.

The Hamiltonian (2) causes two phase errors in each physical block every time it is applied, but the actual damage it does to an encoded state turns out to depend on the code used, and on the state it acts upon. Two examples are considered in this section.

The evolution operator resulting from (2) is, for a single logical block,

$$U(t) = \prod_{n=1}^{N_c-1} (\cos \delta t + i\sigma_{zn}\sigma_{z,n+1} \sin \delta t) \quad (3)$$

since the Pauli matrices for different qubits commute. Thus, a simple perturbative estimate of the failure probability would be as follows: if it is assumed that each term of the form $\sigma_{zn}\sigma_{z,n+1}$ leads to a distinct (orthogonal) uncorrectable error, there are $N_c - 1$ such terms in (3), and the sum of the squares of their amplitudes is

$$\begin{aligned} P_{pert}(t) &= (N_c - 1) (\cos^2 \delta t)^{N_c-1} \sin^2 \delta t \\ &\simeq (N_c - 1)(\delta t)^2 \end{aligned} \quad (4)$$

for sufficiently small interaction strength and time δt .

As it turns out, this expression is not, in general, correct, even for small δt , because of two assumptions: that all terms of the form $\sigma_{zn}\sigma_{z,n+1}$ lead invariably to fatal (uncorrectible) errors, and that the different errors are orthogonal. This is explored in detail in what follows.

A. The 7-qubit code

Consider the 7-qubit code introduced by Steane [8]:

$$\begin{aligned} |0_L\rangle = \frac{1}{\sqrt{8}}(&|0000000\rangle + |0001111\rangle + |0110011\rangle \\ &+ |0111100\rangle + |1010101\rangle + |1011010\rangle \\ &+ |1100110\rangle + |1101001\rangle) \end{aligned} \quad (5a)$$

$$\begin{aligned} |1_L\rangle = \frac{1}{\sqrt{8}}(&|1111111\rangle + |1110000\rangle + |1001100\rangle \\ &+ |1000011\rangle + |0101010\rangle + |0100101\rangle \\ &+ |0011001\rangle + |0010110\rangle) \end{aligned} \quad (5b)$$

Because the code is non-degenerate, all 7 states of the form $\sigma_{zn}|0_L\rangle$ (with $n = 1, \dots, 7$) are orthogonal to each other and to $|0_L\rangle$. Altogether, then, these eight states form an orthogonal basis of the space spanned by the eight kets appearing in (5a). But then, since any combination of products of σ_{zn} acting on $|0_L\rangle$ does nothing but to change the relative signs in the superposition of these eight kets, it follows that it can always be written as a superposition of “one-error” states:

$$U(t)|0_L\rangle = C_0|0_L\rangle + \sum_{n=1}^7 \sigma_{zn}|0_L\rangle \quad (6)$$

and this is always correctible. A similar reasoning applies to the state $|1_L\rangle$, which means that, if the initial state of the system is either $|0_L\rangle$ or $|1_L\rangle$, the evolution operator (3) does not introduce any fatal errors at all.

On the other hand, the initial state of the system is much more likely to be a coherent superposition of $|0_L\rangle$ and $|1_L\rangle$, and for such states the situation is different, because, although error correction will restore $|0_L\rangle$ and $|1_L\rangle$ separately, it will also introduce a phase difference between them. The following useful relations can be easily established from the explicit forms (5):

$$\begin{aligned} \sigma_{z1}\sigma_{z2}|0_L\rangle &= \sigma_{z5}\sigma_{z6}|0_L\rangle = -\sigma_{z3}|0_L\rangle \\ \sigma_{z2}\sigma_{z3}|0_L\rangle &= \sigma_{z4}\sigma_{z5}|0_L\rangle = \sigma_{z6}\sigma_{z7}|0_L\rangle = -\sigma_{z1}|0_L\rangle \\ \sigma_{z3}\sigma_{z4}|0_L\rangle &= -\sigma_{z7}|0_L\rangle \end{aligned} \quad (7a)$$

$$\begin{aligned} \sigma_{z1}\sigma_{z2}|1_L\rangle &= \sigma_{z5}\sigma_{z6}|1_L\rangle = \sigma_{z3}|1_L\rangle \\ \sigma_{z2}\sigma_{z3}|1_L\rangle &= \sigma_{z4}\sigma_{z5}|1_L\rangle = \sigma_{z6}\sigma_{z7}|1_L\rangle = \sigma_{z1}|1_L\rangle \\ \sigma_{z3}\sigma_{z4}|1_L\rangle &= \sigma_{z7}|1_L\rangle \end{aligned} \quad (7b)$$

and it is easily seen from this that when error correction is applied to the state $\sigma_{zn}\sigma_{z,n+1}(\alpha|0_L\rangle + \beta|1_L\rangle)$, the result will be the state $(-\alpha|0_L\rangle + \beta|1_L\rangle)$, that is, a state with the wrong relative phase. Equations (7) also show that the assumption that different $\sigma_{zn}\sigma_{z,n+1}$ lead to orthogonal error states is incorrect: for instance, $\sigma_{z1}\sigma_{z2}$ and $\sigma_{z5}\sigma_{z6}$ lead to the same error state.

Using Eqs. (7) it is straightforward to derive the correct form of the approximate failure probability for small δt . When only the terms of first order in δt are kept in the expression (3), acting on a general state $\alpha|0_L\rangle + \beta|1_L\rangle$, one obtains

$$\delta t (3\sigma_{z1} + 2\sigma_{z3} + \sigma_{z7})(-\alpha|0_L\rangle + \beta|1_L\rangle) \quad (8)$$

which means that the probability that after error correction one might end up with the state $-\alpha|0_L\rangle + \beta|1_L\rangle$ is $(3^2 + 2^2 + 1^2)(\delta t)^2 = 14(\delta t)^2$. One might directly call this the failure probability (since the state $-\alpha|0_L\rangle + \beta|1_L\rangle$ is generally not equal to the initial state $\alpha|0_L\rangle + \beta|1_L\rangle$) or define the failure probability as including explicitly the square of the overlap between the initial and the final state (see Eq. (10), below, for the precise definition), in which case one finds

$$P \simeq 14(\delta t)^2 \left(1 - \left(|\alpha|^2 - |\beta|^2 \right)^2 \right) \quad (9)$$

where the \simeq sign is a reminder that this is only valid for small δt . The failure probability (9) is largest for the symmetric linear superpositions $(|0_L\rangle \pm |1_L\rangle)/\sqrt{2}$. Note how it is different from the result (4) (for $N_c = 7$), obtained under the assumption that the errors generated by different $\sigma_{zn}\sigma_{z,n+1}$ were all orthogonal, and it is also not equal to the same expression with $N_c - 1$ replaced by $(N_c - 1)^2$, which would correspond to a “worst case scenario” in which all the different errors added coherently. The coefficient 14 falls instead in between the two extremes of 6 ($N_c - 1$) and 36 ($(N_c - 1)^2$).

The definition of the failure probability P used above is

$$P = 1 - |\langle \Psi_0 | U(t) | \Psi_0 \rangle|^2 - \sum_{n=1}^{N_c} |\langle \Psi_0 | \sigma_{z,n} U(t) | \Psi_0 \rangle|^2 \quad (10)$$

that is, one minus the total probability that, after a time t , the system may be found in either the original state $|\Psi_0\rangle$, or one of the N_c correctible states $\sigma_{z,n}|\Psi_0\rangle$ (there are, of course, other correctible states, of the form $\sigma_{x,n}|\Psi_0\rangle$ and $\sigma_{y,n}|\Psi_0\rangle$, but they cannot be accessed by this interaction operator).

Using this definition it is relatively straightforward to calculate P exactly for arbitrarily large δt . The following relation is useful:

$$\langle 0_L | \sigma_{z,n_1}, \dots, \sigma_{z,n_k} U | 0_L \rangle = (-1)^k \langle 1_L | \sigma_{z,n_1}, \dots, \sigma_{z,n_k} U | 1_L \rangle \quad (11a)$$

$$\langle 0_L | \sigma_{z,n_1}, \dots, \sigma_{z,n_k} U | 1_L \rangle = 0 \quad (11b)$$

where $k = 0, \dots, 7$. This follows directly from the fact that U involves always the product of an even number of σ_z operators, and that the code words used in $|0_L\rangle$ are the complementsaries of the ones used in $|1_L\rangle$.

For future use it is convenient to define

$$f_0 = |\langle 0_L | U | 0_L \rangle|^2 = |\langle 1_L | U | 1_L \rangle|^2 \quad (12a)$$

$$f_1 = \sum_{n=1}^7 |\langle 0_L | \sigma_{z,n} U | 0_L \rangle|^2 = \sum_{n=1}^7 |\langle 1_L | U | 1_L \rangle|^2 \quad (12b)$$

Direct calculation then yields

$$f_0 = 1 - f_1 = \cos^2(\delta t) \cos^2(2\delta t) \cos^2(3\delta t) \quad (13)$$

and

$$P(t) = f_1 \left(1 - \left(|\alpha|^2 - |\beta|^2 \right)^2 \right) \quad (14)$$

and it is easy to verify that (9) is the lowest-order term in the expansion of (14) in powers of δt .

The failure probability (14) for the case $|\alpha| = |\beta|$ is plotted in Figure 1 (solid line) as a function of δt , from $\delta t = 0$ to $\pi/2$. From 0 to π , the curve is symmetric about $\pi/2$, as is to be expected from the form of the evolution operator (3).

B. The 5-qubit code

In 1996 Laflamme et al. [9] introduced a 5-qubit code which can correct general one-qubit errors. A possible encoding is

$$\begin{aligned} |0_L\rangle &= \frac{1}{\sqrt{8}}(-|00000\rangle + |01111\rangle - |10011\rangle + |11100\rangle \\ &\quad + |10101\rangle + |11010\rangle + |00110\rangle + |01001\rangle) \end{aligned} \quad (15a)$$

$$\begin{aligned} |1_L\rangle &= \frac{1}{\sqrt{8}}(-|11111\rangle + |10000\rangle + |01100\rangle - |00011\rangle \\ &\quad - |01010\rangle - |00101\rangle + |11001\rangle + |10110\rangle) \end{aligned} \quad (15b)$$

The codewords can be obtained from the 7-qubit code by deleting any two qubits (in this case, the first two), but the pattern of signs is nontrivial.

Note that the logical 0 and 1 states are still superpositions of eight basis vectors each (where the basis vectors are simultaneous eigenstates of all the $\sigma_{z,n}$); hence, the ten one-error states $\sigma_{z,n}|0_L\rangle$ and $\sigma_{z,n}|1_L\rangle$, plus the two no-error states $|0_L\rangle$ and $|1_L\rangle$ are not enough to span the space resulting from all the possible combinations of the 16 basis kets. As a result, there are now no states which exhibit fully correctible evolution (unlike the $|0_L\rangle$ and $|1_L\rangle$ did for the 7-qubit code). However, we still have the phenomenon of non-orthogonal errors. In particular, we find that

$$\sigma_{z2}\sigma_{z3}|0_L\rangle = \sigma_{z4}\sigma_{z5}|0_L\rangle \quad (16a)$$

$$\sigma_{z2}\sigma_{z3}|1_L\rangle = \sigma_{z4}\sigma_{z5}|1_L\rangle \quad (16b)$$

and neither of these expressions is equivalent to a linear combination of single-qubit errors acting on $|0_L\rangle$ or $|1_L\rangle$; in fact, they are orthogonal to all such states, and to the no-error states $|0_L\rangle$ and $|1_L\rangle$ as well.

The calculation of $P(t)$, as given by the definition (10) is a little more involved, although the results (11) still hold. Defining as before

$$f_0 = |\langle 0_L | U | 0_L \rangle|^2 = |\langle 1_L | U | 1_L \rangle|^2 \quad (17a)$$

$$f_1 = \sum_{n=1}^5 |\langle 0_L | \sigma_{z,n} U | 0_L \rangle|^2 = \sum_{n=1}^5 |\langle 1_L | U | 1_L \rangle|^2 \quad (17b)$$

one finds, thanks to Eqs. (11), that $P(t)$ can still be written as

$$P(t) = 1 - f_0 - f_1 (\lvert\alpha\rvert^2 - \lvert\beta\rvert^2)^2 \quad (18)$$

but this time, unlike for the 7-qubit code, one does not have $f_0 = 1 - f_1$. Instead,

$$f_0 = \cos^4(\delta t) \cos^2(2\delta t) \quad (19a)$$

$$f_1 = \sin^2(\delta t) (1 + \cos^2(\delta t) \cos^2(2\delta t)) \quad (19b)$$

The failure probability (18) for the case $\lvert\alpha\rvert = \lvert\beta\rvert$ is plotted in Figure 2 (solid line) as a function of δt , from $\delta t = 0$ to $\pi/2$. For small values of δt Eq. (18) reduces to

$$P \simeq (\delta t)^2 \left[6 - 2 (\lvert\alpha\rvert^2 - \lvert\beta\rvert^2)^2 \right] \quad (20)$$

The reason $f_0 \neq 1 - f_1$ for the 5-qubit code is that, as mentioned above, the states $|0_L\rangle$ and $\sigma_{z,n}|0_L\rangle$ do not form a complete basis of the space spanned by the eight kets which make up $|0_L\rangle$. For the 7-qubit code, instead, they do, and, since the operator U acts entirely within that space (when the initial state is $|0_L\rangle$), any part of $U|0_L\rangle$ which is not accounted for by the original state $|0_L\rangle$ has to show up in one of the $\sigma_{z,n}|0_L\rangle$ (and the same for the initial state $|1_L\rangle$).

III. CONCATENATED CODES

A relatively straightforward way to obtain a code that can correct more than one-qubit errors is to concatenate a one-error correcting code, in principle, as many times (or levels deep) as necessary [6,7]. In a code concatenated once, each logical qubit consists of N_c blocks of N_c (lower-level) qubits each. This code can protect against general errors in any three lower-level qubits, and also against many other combinations of multiple lower-level errors. The minimum number of lower-level errors required to cause the code to fail is four, two in one upper level block (causing that whole block to fail) and two in a different one.

In this section I look first at the 7-qubit and 5-qubit codes concatenated once. A physical (lowest-level) qubit will be identified by two indices, n and m , running from 1 to N_c : the first index denotes the upper-level block it belongs to, and the second index the qubit's position within that block. With the assumption that different blocks do not interact, the time-evolution operator (3) becomes

$$U(t) = \prod_{n=1}^{N_c} \prod_{m=1}^{N_c-1} (\cos \delta t + i\sigma_{nm}\sigma_{n,m+1} \sin \delta t) \quad (21)$$

From now on, for simplicity, the subscript z on σ_z will be dropped, as only σ_z is used.

A. The 7-qubit code

If all the errors generated by the individual terms in (21) were orthogonal, it would be a relatively simple matter to calculate the probability of an uncorrectable error to lowest order. It would be given by the terms of the form $\sigma_{n_1 m_1} \sigma_{n_1, m_1 + 1} \sigma_{n_2 m_2} \sigma_{n_2, m_2 + 1}$, with $n_1 \neq n_2$ and m_1, m_2 arbitrary. There are $C(N_c, 2)$ ways to choose the indices n_1 and n_2 , and for each choice there are $(N_c - 1)^2$ different ways to choose m_1, m_2 , so there is a total of

$$\binom{N_c}{2} (N_c - 1)^2 \quad (22)$$

terms in (21) which contribute to the failure probability in lowest order, and all these terms are proportional to $(\delta t)^4$ (after squaring the probability amplitudes).

However, as has been shown already in the previous section, not all the terms enumerated in (22) are mutually orthogonal. For the 7-qubit code, according to (7), there are two sets of values for m_1 (one set of three values, and one set of two values) which result in identical states. When the equivalent choices for m_2 are factored in and added, and the probability amplitudes of the corresponding states are squared, one finds, instead of the factor $(N_c - 1)^2 = 36$ in (22), a factor

$$(3^2 + 2^2 + 1^2)(3^2 + 2^2 + 1^2) = 14^2 = 196 \quad (23)$$

As a result, to lowest order, the failure probability for this two-level code is given by

$$\begin{aligned} P^{(2)} &\simeq 196 \binom{7}{2} (\delta t)^4 \left(1 - (|\alpha|^2 - |\beta|^2)^2 \right) \\ &= 4116 (\delta t)^4 \left(1 - (|\alpha|^2 - |\beta|^2)^2 \right) \end{aligned} \quad (24)$$

for a state $\alpha|0_L\rangle + \beta|1_L\rangle$. The dependence on α and β exhibited by (24) may not be immediately obvious at this point (it will be derived later), but it shows that, for the concatenated code also, the individual states $|0_L\rangle$ and $|1_L\rangle$ are fully correctible.

Note that the maximum error probability $P_{max}^{(2)}$ for the once-concatenated code, according to (24), is related to the corresponding one for the plain code, (9), by the formula

$$P_{max}^{(2)} = \binom{7}{2} (P_{max}^{(1)})^2 \quad (25)$$

and the right-hand side of (25) is simply the probability that two blocks might fail *independently*, times the number of ways to choose two blocks. This is because, to this order (recall that these are only approximate results for small δt), errors across different blocks are orthogonal, ie., they add incoherently. This can also be seen from Equation (23): within each block there is some coherent addition of error amplitudes (which results in the terms 3^2 and 2^2), but then the total error probabilities for each block are simply multiplied.

This is an important result which generalizes to higher orders, as discussed later in this Section (subsection C). The key point is that all the errors which would cause a particular block to fail are orthogonal to all the errors that would cause a *different* block to fail, *to lowest order*. This is because to lowest order all it takes is two errors in one block to cause that block to fail, and because the original code is nondegenerate, which means that all expectation values of the form $\langle \xi_L | \sigma_i \sigma_j | \eta_L \rangle$ (where $\eta, \xi = 0, 1$) within the same block are zero.

Equation (25) does not, however, hold for arbitrarily large δt , when multiple (more than two) errors within the same block need to be taken into account. For a code concatenated only once it is still possible, albeit very cumbersome, to derive this failure probability for arbitrary δt . The definition (10) has to be changed to

$$P = 1 - |\langle \Psi_0 | U(t) | \Psi_0 \rangle|^2 - \sum_n |\langle \Psi_0 | A_n U(t) | \Psi_0 \rangle|^2 \quad (26)$$

where the $\{A_n\}$ represent a maximal set of correctible error operators leading to orthogonal states. The difficulty is that now, unlike in the previous Section, not all possible correctible errors lead to orthogonal states. For instance, any number of errors within one single block are now correctible, but certainly not all of these lead to orthogonal states. Thus, even though we started out with a nondegenerate code, *the concatenated code is degenerate* [10].

As far as I can tell, the set $\{A_n\}$ in (26) must be constructed by inspection. For the 7-qubit code, concatenated once, I find that the maximum number of correctible errors acting on a single block and leading to orthogonal states is 15, which can be chosen to be

$$\begin{aligned} \sigma_{nm} & \quad (m = 1, \dots, 7) \\ \sigma_{n1} \sigma_{nm} & \quad (m = 2, \dots, 7) \\ & \quad \sigma_{n2} \sigma_{n3} \\ & \quad \sigma_{n1} \sigma_{n4} \sigma_{n5} \end{aligned} \quad (27)$$

Of these, the first 7 are, of course, fully correctible at the lower level, whereas the others, upon correction at the lower level, lead to what look like “block” phase errors at the higher level.

The single-block errors (27) can be combined in a large number of ways among the different blocks to yield other, orthogonal, correctible errors. Fortunately, however, the actual number of such combinations which make a nonvanishing contribution to (26) is relatively small. To see this, divide the error operators acting on a single block into those involving an even number of σ 's (denoted as E_n if they act on the n -th block) and those involving an odd number of σ 's (denoted as O_n). Then, for a general multiblock error of the form $A = E_{n_1} \dots E_{n_k} O_{m_1} \dots O_{m_k}$, Eqs. (11) for a single block imply that the expectation value

$$\langle 0_L | O_{n_1} \dots O_{n_k} E_{m_1} \dots E_{m_l} U | 0_L \rangle \quad (28)$$

will only be nonzero if the corresponding combination $\langle 0_L | \sigma_{n_1} \dots \sigma_{n_k} | 0_L \rangle$ is nonzero for the single, non-concatenated, code. The same is true for the state $|1_L\rangle$, and there are no cross-terms between $|0_L\rangle$ and $|1_L\rangle$ (also as a direct consequence of the single-block Eqs. (11)). Thus, to evaluate (26), it is sufficient to identify the combinations of numbers $\{n_1, \dots, n_k\}$ which lead to a nonzero $\langle 0_L | \sigma_{n_1} \dots \sigma_{n_k} | 0_L \rangle$ for the 7-qubit code, and put odd errors, chosen from the list (27), in the blocks n_1, \dots, n_k , augmented perhaps with even errors, always chosen from the list (27), in any other blocks, provided, of course, that the total error be correctible. This quickly reduces the total of different possibilities to a manageable number: for instance, since an even error in one block would cause that block to fail, one cannot have even errors in more than one block at a time.

For reference, for the 7-qubit code, the sets of values of n_1, \dots, n_k to be used are: $(1, 2, 3)$, $(1, 4, 5)$, $(1, 6, 7)$, $(2, 4, 6)$, $(2, 5, 7)$, $(3, 4, 7)$, $(3, 5, 6)$, the complementary set $((4, 5, 6, 7)$, $(2, 3, 6, 7)$, and so on), and the set $(1, 2, 3, 4, 5, 6, 7)$. Then, possible error operators A_n to be used in (26) might be products such as such as $\sigma_{1,m_1}\sigma_{2,m_2}\sigma_{3,m_3}$, or $\sigma_{1,m_1}\sigma_{2,m_2}\sigma_{3,m_3}\sigma_{4,1}\sigma_{4,m_4}$, or $\sigma_{n,1}\sigma_{n,m}$. In terms of the functions f_0 , f_1 defined in (12), the term(s) $\sum_{m_1, m_2, m_3} |\langle 0_L | \sigma_{1,m_1}\sigma_{2,m_2}\sigma_{3,m_3} | 0_L \rangle|^2$ contribute a term $f_0^4 f_1^3$ to the expression (26); the term $\sum_{m_1, m_2, m_3, m_4} |\langle 0_L | \sigma_{1,m_1}\sigma_{2,m_2}\sigma_{3,m_3}\sigma_{4,1}\sigma_{4,m_4} | 0_L \rangle|^2$ contributes a term $f_0^3 f_1^4$ (since the product of two σ 's in the same block is equivalent, except for a sign, to a single σ acting on the appropriate state, cf. Eqs. (7)), and so on.

Collecting all the terms, and keeping track carefully of which ones have opposite signs in the states $|0_L\rangle$ and the states $|1_L\rangle$, one finds

$$P^{(2)}(t) = \left(1 - f_0^7 - 7f_0^6 f_1 - 28f_0^4 f_1^3 - 7f_0^3 f_1^4 - 21f_0^2 f_1^5\right) \left(1 - (|\alpha|^2 - |\beta|^2)^2\right) \quad (29)$$

with f_0 and f_1 given by (13), which does reduce to (24) for small δt .

The exact result (29) is plotted as a function of δt in Figure 1 (dashed line), for $|\alpha| = |\beta|$. It is, perhaps, remarkable that it does not look all that different from the single-encoding result (14), except in the very small δt region. It is also clear that Eq. (25) does not hold for large δt , which means that for large δt we do see the effects of errors across different blocks adding coherently.

B. The 5-qubit code

For the 5-qubit code, one again has to identify the appropriate maximal set of error operators leading to orthogonal errors. For a single block, one finds the following set of 15:

$$\begin{aligned} \sigma_{nm} & \quad (m = 1, \dots, 5) \\ \sigma_{n1}\sigma_{nm} & \quad (m = 2, \dots, 5) \\ \sigma_{n2}\sigma_{nm} & \quad (m = 3, \dots, 5) \\ \sigma_{n1}\sigma_{n2}\sigma_{nm} & \quad (m = 3, \dots, 5) \end{aligned} \quad (30)$$

As in the previous subsection, it is found that only certain combinations of odd errors across different blocks lead to nonzero contributions to (26). These turn out to be much fewer than before, being limited to $n_1, \dots, n_k = (1, 2, 5), (1, 3, 4)$, and $(2, 3, 4, 5)$.

The result, valid for arbitrarily large δt , turns out to be now

$$\begin{aligned} P^{(2)}(t) = & 1 - (f_0^5 + 5f_0^4(1-f_0) + f_1^4 + 4f_0f_1^3(1-f_1)) \\ & - (4f_0f_1^3 + 6f_0^2f_1^2 - 8f_0^2f_1^3) \left(|\alpha|^2 - |\beta|^2\right)^2 \end{aligned} \quad (31)$$

with f_0 and f_1 given by Eqs. (19). The factors of $1-f_0$ appearing in (31) come from the sum of the single-block expectation values squared of $\sigma_1\sigma_m$, $m=2,\dots,5$ and $\sigma_2\sigma_m$, $m=3,\dots,5$; these seven error operators, acting on the singly encoded $|0_L\rangle$ or $|1_L\rangle$, generate the seven orthogonal states necessary to complete a basis of the space spanned by the 8 kets appearing in (15). The factors of $1-f_1$ come from the sum of the single-block expectation values squared of $\sigma_1\sigma_2\sigma_m$, $m=3,\dots,5$: these 3 error operators turn out to be the complement of the 5 ones appearing in the definition (16b) of f_1 .

The limit of (31) for small δt is

$$P^{(2)}(t) \simeq (\delta t)^4 \left[360 - 24 \left(|\alpha|^2 - |\beta|^2 \right)^2 \right] \quad (32)$$

As usual, the failure probability is largest for the symmetric superposition state $(|0_L\rangle \pm |1_L\rangle)/\sqrt{2}$. The corresponding coefficient, 360, can be obtained also from the simple arguments used to derive the result (24) in the previous subsection: it equals $C(5, 2)(2^2+1^2+1^2)^2$, where the 2^2 stands for the amplitude square of the sum of the two error terms which lead to identical errors, as shown in Eq. (16) (and the two 1^2 stand for the other two orthogonal errors).

The exact result (31) is plotted in Figure 2 (dashed line) as a function of δt , for $|\alpha|=|\beta|$. In this case, unlike for the 7-qubit code, the difference with the single-encoding formula (solid line, equation (18)) is substantial; the twice-encoded qubit has a substantially smaller failure probability for most values of δt . The failure probability actually goes to zero at $\delta=\pi/2$, where Eq. (21) yields $U=i\prod_{n=1}^5\sigma_{n1}\sigma_{n5}$. Upon inspection, it is found to be a peculiarity of the concatenated (two-levels deep) 5-qubit code that

$$\prod_{n=1}^5 \sigma_{n1}\sigma_{n5} (\alpha|0_L\rangle + \beta|1_L\rangle) = \sigma_{11}\sigma_{15}\sigma_{22}\sigma_{32}\sigma_{42}\sigma_{52} (\alpha|0_L\rangle + \beta|1_L\rangle) \quad (33)$$

and the state on the right-hand side of (33) is fully correctible, since it amounts to only one block failing.

C. Results for arbitrarily deep concatenation

Clearly, the exact calculation of $P^{(n)}$ for a code concatenated n levels deep, with $n>2$, becomes much too cumbersome to be feasible. However, the results in the previous subsections show that the leading term in δt can be calculated using relatively simple arguments.

Consider, for instance, a code concatenated three levels deep. It will fail if at least two of the high-level qubits fail, but these high-level qubits are themselves two-level deep codes. One can choose the two highest-level qubits that fail in any of $C(N_c, 2)$ ways, and for each of them the number of terms in the expansion of the evolution operator which lead to a

qubit failure are those computed for the previous level. So, for the 7-qubit code, we can immediately iterate (24) to get

$$\begin{aligned} P_{max}^{(3)} &\simeq \binom{7}{2} (4116(\delta t)^4)^2 \\ &\simeq \binom{7}{2} (P_{max}^{(2)})^2 \end{aligned} \quad (34)$$

where the subscript “max” indicates that we are looking at the failure probability for the state that maximizes it (the linear combination $(|0_L\rangle \pm |1_L\rangle)/\sqrt{2}$), and Eq. (9) has been used for $P^{(1)}$.

Equation (34) contains the essence of a recursion relation which yields the failure probability at the n -th level of concatenation ($n \geq 2$) as

$$P_{max}^{(n)} \simeq \binom{7}{2}^{-1} \left(\binom{7}{2} P_{max}^{(1)} \right)^{2^{n-1}} \quad (35)$$

Figure 3 shows the approximate $P^{(n)}$, calculated from (35), for $n = 1, \dots, 4$ (solid lines), and also the exact results (14) and (29), for comparison. Based on these examples, it would seem that Equation (35) overestimates the failure probability, which would make it a somewhat conservative estimate

As encoding depth n increases, the failure probability (35) will, for a given δt increase or decrease depending on whether $C(7, 2)P_{max}^{(1)}$ is greater than or less than one. This yields the “threshold” value for $(\delta t)^2$, below which virtually error-free operation can be achieved for sufficiently deep encoding. Using (9), one finds the condition:

$$(\delta t)^2 < \frac{1}{21 \cdot 14} = 3.4 \times 10^{-3} \quad (36)$$

(Figure 3 shows this as the point where all the curves cross.) This threshold (36) is comparable to some estimates for the correction of independent, random errors by concatenate codes, if one thinks of $(\delta t)^2$ as a sort of failure probability for a single physical qubit. As pointed out in the Introduction, this is a natural interpretation (in spite of the fact that two physical qubits at a time are modified by this interaction), because of the result (1).

A similar calculation yields the threshold result for the 5-qubit code (using (20) and $C(5, 2) = 10$):

$$(\delta t)^2 < \frac{1}{10 \cdot 6} = 1.7 \times 10^{-2} \quad (37)$$

IV. DISCUSSION

The results in the previous section suggest that, in principle, the correction of even rather large undesired interactions between the qubits does not require special methods or resources beyond those needed to control independent, random errors arising from the interaction of the qubits with the environment. This observation is based, first, on the fact that estimates

of the threshold for fault-tolerant computation with independent environmental errors tend to be rather more restrictive than either (36) or (37) [6,7]; and, second, on the fact that for most proposed quantum computing systems the unwanted interactions between qubits would easily satisfy the threshold conditions (36) or (37), provided that the time in between error corrections is not excessive.

As an example, consider a system of nuclear spins, in a solid, for instance (such as in the proposal by Kane [11]), separated by $\sim 150 \text{ \AA}$, and interacting via the magnetic dipole-dipole interaction, which would naturally lead to a Hamiltonian like (2). For such a system δ may be estimated as

$$\delta \sim \frac{\mu_0 \mu_N^2}{4\pi \hbar d^3} \sim 10^{-2} \text{ s}^{-1} \quad (38)$$

Here μ_N is the nuclear magneton.

Without error correction δt becomes already of the order of 1 after 100 s, and long calculations are impossible. But assume that one uses error correction and that complete error correction of an n -order encoded qubit requires a time $t = c_n \tau_{gate}$, where the time needed to perform an elementary logic gate for this system is about $\tau_{gate} = 10^{-5} \text{ s}$. Then the threshold is easily reached unless c_n is exceptionally large, which would make error correction generally impossible anyway (a large c_n would mean essentially that the computer architecture does not allow for a large degree of parallelism when correcting errors across different qubits).

Of course, the results presented here have been obtained only for a specific kind of interaction Hamiltonian and a specific geometry, and would need to be modified for other cases (e.g., two-dimensional geometries, with more nearest-neighbors per qubit, or to include non-nearest neighbor interactions). There is also the simplifying assumption made from the outset, of neglecting interactions between qubits in different blocks. These complications might require recalculations for specific physical systems and hardware configurations, but I do not expect them to change substantially the threshold estimates of the previous Section.

For instance, for the kind of “linear” geometry considered here, including interactions between the last qubit of one block and the first one of the next block would not modify the failure probability to lowest order, since a single two-qubit error which straddles two blocks does not cause either block to fail; hence, to make any one block fail, more of these errors are required than of the kind of “internal” errors considered in this paper.

The key result of Section III concerning the incoherent addition of failure probabilities for different blocks, to lowest order, should be quite general: it depends only on the base code being a nondegenerate distance 3 code and the interaction Hamiltonian being a sum of pairwise products of elementary error operators for individual qubits.

The most important “real-life” complication which has been ignored here is, rather, the fact that, in practice, error correction will not be a clean and purely mathematical operation, but a physical one, involving interacting systems and therefore itself subject to error. The theory of fault-tolerant error correction has shown that even when this is accounted for it should still be possible to achieve “almost” perfect error correction, provided that the error rate per gate is below a certain threshold, but it is here where one finds the (possibly) very small error thresholds which constitute the main challenge for large-scale quantum computing.

I am grateful to R. Laflamme and D. A. Meyer for comments. This research has been sponsored by the National Science Foundation and by the Army Research Office.

REFERENCES

- [1] J. Gea-Banacloche, Phys. Rev. A **57**, R1 (1998).
- [2] J. Gea-Banacloche, Phys. Rev. A **60**, 185 (1999).
- [3] This was done, for instance, by Garg, Phys. Rev. Lett. **77**, 964 (1996)
- [4] See, for instance, L. Viola and S. Lloyd, Phys. Rev. A **58**, 2733 (1998)
- [5] D. G. Cory, A. F. Fahmy and T. F. Havel, Proc. Natl. Acad. Sci. USA **94**, 1634 (1997);
N. A. Gershenfeld and I. L. Chuang, Science **275**, 350 (1997).
- [6] J. Preskill, Proc. Roy. Soc. Lond. A **454**, 385 (1998).
- [7] E. Knill, R. Laflamme and W. H. Zurek, Science **279**, 342 (1998).
- [8] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996). See also A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
- [9] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
- [10] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
- [11] B. E. Kane, Nature **393**, 133 (1998).

FIGURES

FIG. 1. The maximum failure probability for a qubit encoded with the plain 7-qubit code (solid line) and with the same code concatenated once (dashed line) as a function of the product of interaction strength and interaction time

FIG. 2. The maximum failure probability for a qubit encoded with the 5-qubit code (solid line) and with the same code concatenated once (dashed line) as a function of the product of interaction strength and interaction time

FIG. 3. Approximate results, valid for small δt , for the maximum failure probability for a qubit encoded with the 7-qubit code concatenated 1 (no concatenation), 2, 3, and 4 levels deep (solid lines). The exact results (from Figure 1) for the cases 1 and 2 are shown as dashed lines.